EP 1 152 368 (3)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/93503 A2

(51) International Patent Classification[7]: H04L 12/18

(21) International Application Number: PCT/US01/40820

(22) International Filing Date: 31 May 2001 (31.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/208,349 31 May 2000 (31.05.2000) US

(71) Applicant *(for all designated States except US)*: **SNIP, LLC** [US/US]; Suite 1670, 300 Esplanade Drive, Oxnard, CA 93030 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **SPURGIN, Ryan, H.** [US/US]; 700 Albany Avenue, Ventura, CA 93004 (US).

(74) Agents: **OH, Sung, I.** et al.; Squire, Sanders & Dempsey L.L.P., 14th Floor, 801 South Figueroa Street, Los Angeles, CA 90017-5554 (US).

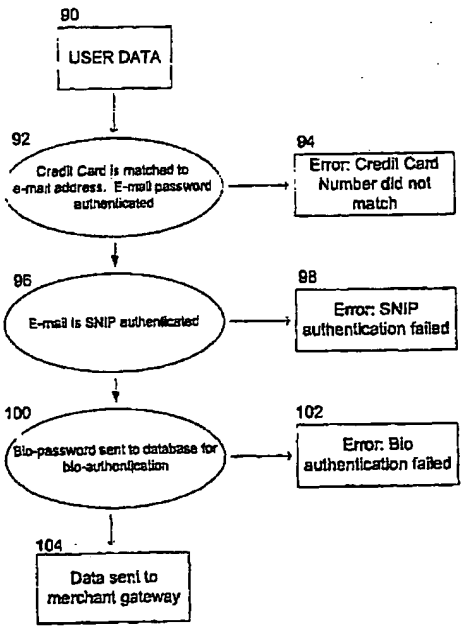
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR LINKING ANY INSTANT MESSAGE SYSTEM AND DATA TRANSFER TECHNOLOGIES



(57) Abstract: The present invention provides a method and system to facilitate peer-to-peer instant message communications among users connected to different instant messaging systems. To do so, the present invention provides a Single Name Instant Messaging Protocol (SNIP) that uses the universal namespace of e-mail to facilitate peer-to-peer instant message communications among users connected to different networks. Another aspect of the present invention is to use the Single Name Instant Messaging protocol to authenticate a user over the Internet to provide online fraud protection when using a credit card. To do so, a method and system according to one embodiment of the present invention includes a database that references a credit card number with an e-mail address and its corresponding e-mail password; and, optionally, referencing the same e-mail address to a bio-rhythmically encoded password.

WO 01/93503 A2

METHOD AND SYSTEM FOR LINKING ANY INSTANT MESSAGE SYSTEM AND DATA TRANSFER TECHNOLOGIES

BACKGROUND OF THE INVENTION

[0001] **1. Field of the Invention:**

[0002] This invention relates generally to a method and system for using a Single Name Instant Messaging Protocol (SNIP) that uses the universal namespace of e-mail to facilitate peer-to-peer instant message communications and/or data communication among users connected to different networks; and using similar protocol to authenticate use of a credit card.

[0003] **2. Description of the Related Art:**

[0004] Even with many technological advances in the Internet, there still are many problems associated with it. For instance, instant messaging is a type of electronic communication that enables a user to chat instantly with one or more individuals via computer. Typically, the instant messaging system alerts the user whenever somebody on the user's private list is online. The user can then initiate a chat session with that particular individual. Unfortunately, there are several competing instant messaging systems and no standard protocol. As a result, for a user to send instant messages to another user, both users must use the same instant messaging system. In other words, two users using different instant messaging systems cannot communicate with each other. Still another shortcoming with the present instant message communication is that each individual instant messaging service maintains separate and limited-capacity namespace of which two parties need to be a member to communicate via instant messages. Thus, this too makes instant messaging across multiple networks difficult, if not impossible.

[0005] Yet another problem associated with the Internet is fraudulent use of a credit card. For instance, just about anyone with credit card information can purchase an item through the Internet without the permission of the owner of the credit card. As such, many credit card users are reluctant to use the credit card through the Internet in fear of the credit card information being stolen when used through the Internet.

[0006] Therefore, there is a need for a method and/or system to allow users to facilitate peer-to-peer instant message communication among users connected to different instant messaging systems and allow protection against fraudulent use of credit cards through the Internet.

BRIEF SUMMARY OF THE INVENTION

[0007] One aspect of the present invention is to provide a method and system to facilitate peer-to-peer instant message communications among users connected to different (and the like) instant messaging systems. To do this, the present invention provides a Single Name Instant

Messaging Protocol (SNIP) that uses the universal namespace of e-mail to facilitate peer-to-peer instant message communications among users connected to different networks. Under this protocol, a user can register its e-mail address and Internet Protocol (IP) address with a SNIP server. If another member wishes to communicate with a target user by instant messages, the member sends an authentication request to the SNIP server. The SNIP server forwards that authentication request to the target user's e-mail server, such as POP3, a commonly used e-mail protocol, detailed in RFC 1939. If the SNIP server receives proper acknowledgment from the user's mail server, the target user is registered with the SNIP server as being "online." Then instant message communication can commence. Alternatively, the present invention may use IMAP (Internet Message Access Protocol), another commonly used e-mail protocol, to authenticate a user. For protocols other than POP and IMAP, authentication may be accomplished in a slightly different manner.

[0008] By way of background, authentication may be defined as the process of proving the identity of an individual, usually based on a user name and/or password. Moreover, POP may be generally defined as a protocol used to retrieve an e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can also use the newer IMAP (Internet Message Access Protocol). There are two versions of POP. The first, called POP2, became a standard in the mid-80's and requires SMTP (Simple Mail Transfer Protocol) to send messages. The newer version, POP3, can be used with or without SMTP, which is a lower level mail protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. For this reason, a user generally needs to specify both the POP or IMAP server and the SMTP server when the user configures its e-mail application.

[0009] With the SNIP system, substantially all, if not all, users registered with the SNIP server have the ability to receive instant messages through their e-mail address or IP number regardless of the ISP (Internet Service Provider) or online service to which they belong.

[0010] Another aspect of the present invention is to use the e-mail address verification of the Single Name Instant Messaging protocol to authenticate a user over the Internet to provide online fraud protection when using a credit card. To do so, a method and system according to one embodiment of the present invention includes a database that references a credit card number with an e-mail address and its corresponding e-mail password; and, optionally, referencing the same e-mail address to a bio-rhythmically encoded password. For instance, once the credit card number is registered with the corresponding e-mail address, and e-mail password, and optionally

the bio-password, an exemplary protection against fraudulent use of a credit card may be provided as follows. To make a purchase online, all of the typical consumer information is filled out; but before approval of the credit card purchase, the system, according to the present invention first checks the credit card number against the e-mail address matching the credit card. Secondly, the system checks the e-mail password to see if it matches the password for the e-mail address corresponding to the credit card. Thereafter, the system may optionally check the bio-rhythmic values of the encoded bio-read of the e-mail password against the bio database for the e-mail password in SNIP, for example. If all of the above succeeds, then the online transaction may go to the gateway for possible clearing. On the other hand, if any one of the above verifications do not match, then the cardholder is prevented from proceeding with the online transaction.

[0011] With regard to verifying the identity of the credit card user using its bio-rhythm, U.S. Patent No. 4,805,222 entitled "Method and Apparatus for Verifying an Individual's Identity," issued to Young, et al. on February 14, 1989, is hereby incorporated by reference into this application.

[0012] The above described and many other features and attendant advantages of the present invention will become apparent from a consideration of the following detailed description when considered in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] A detailed description of the preferred embodiment of the invention will be made with reference to the accompanying drawings;

[0014] FIG 1is an exemplary flow chart illustrating the procedure for a SNIP client to log onto and authenticate with the SNIP server;

[0015] FIG. 2 is an exemplary flow chart illustrating the procedure for a SNIP client to look up another user with the SNIP server;

[0016] FIG. 3 is an exemplary block diagram of a SNIP server facilitating peer-to-peer instant message communications and/or data communication among users connected to different networks;

[0017] FIG. 4 is an exemplary message board to facilitate peer-to-peer communication; and

[0018] FIG. 5 is an exemplary flow chart for an authentication procedure.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0019] This description is not to be taken in a limiting sense, but is made merely for the purpose of illustrating the general principles of the invention. The section titles and overall organization of the present detailed description are for the purpose of convenience only and are not intended to limit the present invention.

[0020] One aspect of the present invention is to provide a Single Namespace Instant Messaging Protocol (SNIP) to facilitate peer-to-peer, client-to-server instant message communications and/or data communication among users connected to different networks. One of the advantages with SNIP is that it uses existing networks for authentication by using existing universal namespace, i.e., the e-mail address of users. Since all of these networks are already established, the present invention uses the existing foundation for authentication and registration. For example, by using POP3 protocol RFC #1725, SNIP can authenticate a user from any network that has an Internet e-mail address. After the server authenticates and registers the user's e-mail address and IP, then the client is ready for peer-to-peer and/or client-to-server and/or three-tier communications.

[0021] In the following description, the term "client" generally denotes a software and/or source code that handles interaction between a user and a server, and back and forth. For example, a client, sometimes called a client/server architecture, may be a network architecture in which each computer or process on the network is either a client or a server. Servers are computers or processes dedicated to managing disk drives (file servers), printers (printer servers), or network traffic (network servers) and the like. Put differently, clients are PCs or workstations on which users run applications. Clients rely on servers for resources, such as files, devices, and even processing power. Another type of network architecture is known as a peer-to-peer architecture because each node has equivalent responsibilities. Both client/server and peer-to-peer are widely used, and each has unique advantages and disadvantages. Client/server architectures are sometimes called two-tier architectures. In particular, an e-mail client may be an application that runs on a personal computer or workstation and enables the user to send, receive and organize e-mail. It's called a client because e-mail systems are based on client/server architecture as discussed above. Mail is sent from many clients to a central server, which reroutes the mail to its intended destination.

[0022] There is also another type of client/server architecture with three well-defined and separate processes, each running on a different platform: (1) the user interface, which runs on the user's computer (the client); (2) the functional modules that actually process data. This middle tier runs on a server and is often called the application server; and (3) a database management system (DBMS) that stores the data required by the middle tier. This tier runs on a second server called the database server. This three-tier design has many advantages over traditional two-tier or single-tier designs, the chief ones being (a) the added modularity makes it easier to modify or replace one tier without affecting the other tiers; and (b) separating the application functions from the database functions makes it easier to implement load balancing and scalability.

[0023] As illustrated by way of example in FIG. 1, an exemplary SNIP protocol 10 may follow these authentication steps. In step 20, to authenticate, a client sends a POP3 authentication request to the SNIP server. In step 22, the SNIP server forwards that authentication request to the user's e-mail protocol, such as the POP3 server, using RFC number 1725, for example. Note that the POP3 server is used as an example in this embodiment; or other e-mail protocol, such as IMAP or new protocol that may be developed in the future, may be used. In step 24, a SNIP server receives an "ack" or "nack" from the user's POP3 server. Note that the term "ack" generally means that the user's POP3 server acknowledged the authentication request from the SNIP server; and the term "nack" generally means that the user's POP3 server did not acknowledge the authentication request. Here, if a SNIP server receives an "ack" from the user's POP3 server, then the protocol 10 proceeds to step 26, where the user's e-mail address and IP number are registered with the SNIP server as being ON-LINE.

[0024] On the other hand, if the SNIP server receives a "nack" from the user's POP3 server, then the authentication has failed and will return to step 20 for a re-authentication procedure. The user's POP3 may not acknowledge the authentication request for many reasons, such as the IP address not matching, wrong user's name, wrong e-mail address, wrong password, wrong setting for the e-mail server, and the server not running. However, if correct parameters are input for the user, then the POP3 server should acknowledge the authentication request from the SNIP server, i.e., return an "ack" to the SNIP server.

[0025] With the above SNIP authentication procedure and the SNIP protocol 10, all clients/users registered with the SNIP server now have the ability to receive instant messages through their e-mail address and/or IP number, regardless of which ISP or online service to which they belong. The instant messaging, for example, now takes place over peer-to-peer, client-to-client, client-to-server (two-tier), and three-tier connections, freeing the SNIP server from "ack," "nack," and control protocols. That is, once authenticated, to make a peer-to-peer connection, for example, the first client drops the link with the SNIP server automatically, and tries to open a socket with the second client using the IP address and/or e-mail address information for the second client gotten from the SNIP server.

[0026] By way of background, a socket in UNIX and some other operating systems may be generally described as a software object that connects an application to a network protocol. In UNIX, for example, a program can send and receive TCP/IP messages by opening a socket and reading and writing data to and from the socket. This simplifies program development because the programmer need only worry about manipulating the socket and can rely on the operating system to actually transport messages across the network correctly. Moreover, by using POP3 for the authentication procedure, for example, it eliminates the end user from having to go

through a lengthy registration process. This also ensures that SNIP uses a single namespace, and is available to anyone in the world that has an e-mail address that uses POP3 or other useable protocols. Of course, other connection methods known to one skilled in the art may be used with the present invention.

[0027] FIG. 2 illustrates an exemplary procedure for a SNIP client to look up another user with a SNIP server. To do so, the client logs on. The first time the client runs or the user intentionally decides to change its identity, the SNIP server may prompt the client and/or user for its POP3 e-mail name and password. A POP3 connection may be established with its e-mail server, and the e-mail name and address may be verified. This information can then be saved as a new "client profile," to which buddy / ignore / and other data can be added – a nickname, for example. Once the user has logged onto the client, the client may establish a connection to the server, sending the previously validated e-mail name and the IP address of the server on which the client is running.

[0028] Moreover, besides the e-mail and the IP address, the connection may be established with a GUID (Globally Unique ID) to ensure that the client is who the user says it is. GUID may be generally defined as an algorithm that works off a MAC (Machine Address Code) address, which is a government number given to every Ethernet card or hub on the network. That is, users that have Ethernet cards have a unique number so that no other user can have the same GUID. With the present invention, once the client comes online, a GUID may be pinned to the client, which is then sent to the SNIP server, along with the IP address and/or e-mail address, to authenticate. Then, after a peer-to-peer connection is made between two or more clients, the GUID may be used as a secret code between the clients during that session. So if one of the clients drops out of the connection, either intentionally or unintentionally, and a different client by chance is assigned the same IP address of the dropped client, the different client cannot be connected to the session, although the IP address may be the same as the one given by the SNIP server because the GUID of the different client does not match the GUID of the session.

[0029] For example, if a first client and a second client are online and the second client, for some reason, drops off and tries to come back online, the second client may get a new IP address; therefore the first client is unable to connect to the second client because of the different IP address now assigned to the second client. Moreover, if by chance a third client, who was not originally connected to the first client, is now assigned to the IP address which previously belonged to the second client, the first client cannot connect to the third client because the GUID does not match. This way, the first client is not fooled into thinking that the third client is the second client. Rather, to reconnect to the second client, either the first or second clients need to re-authenticate to establish the connection.

[0030] In step 30 of FIG. 2, the client can establish a conversation by indicating the user's e-mail address or the name the user client wants to talk to by sending a look-up request to the SNIP server with the e-mail address of the desired user. In step 32, the SNIP server attempts to find the corresponding IP address by first checking its local cache of addresses. In other words, the SNIP server checks the database for the e-mail address of the desired user. In step 34, if the address is not cached locally, or the attempt to connect to that address fails, then in step 36, the SNIP server may e-mail a notification to the desired user's e-mail box. This is to notify the user of the incoming request for connection. Moreover, in step 38, the SNIP server notifies the original client that the desired user is not available and that an e-mail notification has been sent to the e-mail address. Still further, the e-mail includes a message describing SNIP and a URL (Uniform Resource Locator) to download and install the SNIP protocol. Then, the SNIP server may return to step 30, ready to send another look-up request. Still further, the client may connect to the SNIP server and request the IP address for the given e-mail name. Moreover, if the server responds with an IP address different than the locally cached one, then the client may attempt to connect to this new IP address. Alternatively, the SNIP server can try its own local cache before it queries the SNIP server for an address.

[0031] On the other hand, in step 40, if the connection is successful, the IP address is saved in the local cache. Upon successful connection, the client sends the requesting user's e-mail name and possibly other information, such as nickname, etc. In step 42, once connected, the client can communicate directly with the desired user and bypass the SNIP server by opening a socket using the IP address and/or e-mail address information gotten from the SNIP server. This way, any data may be exchanged between the client and user as they wish. Of course, the above embodiment is not limited to communication between two people, i.e., a client and a user. Rather, it may be used to communicate amongst a plurality of clients and users.

[0032] Therefore, steps 30 to 42 generally describe a procedure for an original client to look up another client with the SNIP server. If the SNIP server has the desired user in its database, then it returns the IP address of the desired user to the original client. If the SNIP server does not have the desired user in its database, the original client is then notified that the desired user cannot be found and that an e-mail was sent to the desired user with notification of the incoming SNIP request.

[0033] Alternatively, when a client receives a conversation request from another client, the receiving user may be prompted to let the user know that another SNIP client is trying to contact the receiving user. Optionally, this alternative feature may be set by the receiving user to "always ignore" or "always accept" the conversation request. If the receiving user rejects the

request, then the receiving user can choose to send a short rejection message along with the rejection.

[0034] Still another embodiment of the present invention is to transfer data between connected clients. That is, once a conversation has begun, the two clients may send messages back and forth. The sending client may establish a connection, send the data, wait for acknowledgment, and then disconnect. A "message header" may precede the message data, describing the type and size of the message data, the time when it was sent, and a checksum for verifying message integrity. "Plain Text," "Formatted Text," "Files," or "Voice" are some examples of formats or data that may be transferred with the present invention. Of course, other data may be transferred using the present invention as known to one skilled in the art.

[0035] Yet another embodiment of the present invention is to provide a periodic pinging of "buddies." For example, the client can establish a list of "buddies" that the client wants to track. The client will periodically try to determine if each "buddy" is on line. To check, the client may try to connect to the target client via the locally cached IP address. If the ping fails, it may request a new IP from the SNIPS server, and update its local cache and try again if it gets one. If the client-to- client "ping" connection is successful, then the user is shown as "on line." If neither succeeds, the person is shown as "off line."

[0036] Still another alternative embodiment of the present invention is to enforce the "ignore." In this embodiment, the client may cache a list of e-mail names and/or IP addresses which the client has chosen to ignore. Having done so, all connection requests from the "ignore" list of e-mail names or IP addresses may be automatically rejected. In particular, the option of ignoring by IP addresses would prevent a user in the "ignore" list from simply changing its e-mail name and bypassing the ignore list. Furthermore, to prevent users using different IP and e-mail names from getting through, a secondary GUID or GUID for that session may be used to enforce the "ignore."

[0037] FIG. 3 illustrates by way of example block diagrams representing the interaction among the main SNIP server 50, SNIP clients 52, and SNIP servers 54. With regard to the main SNIP server 50, it works as a regular SNIP server, but with the added responsibility of directing traffic for other SNIP servers. That is, the main SNIP server 50 handles requests similar to Intetnic and the Whois structure. However, these requests may be searching for SNIP servers. For example, for an ISP to register, a SNIP server may fill out the forms to update the SNIP central database. It may also require a proof of ownership of the domain. When a client searches for a specific user, it first checks the main database. If the main database does not have that person registered, the client then tries to find the secondary SNIP server for that domain name, if

that person is not registered there, then that person is offline. So the main SNIP server keeps a database of current users as well as a database of registered SNIP servers.

[0038] Moreover, the main SNIP server may be implemented as a multi-threaded application. The main thread may be idle, i.e., waiting for TCP/IP connections on the designated server port. Upon receiving a connection, the server may spawn a child thread to handle the transaction, then return to its wait state. The child thread may then handle the transaction with the connecting client, which may be one of two types, a "register" transaction, or a "get address" transaction. In general, the register transaction is where the client sends an e-mail name and IP address so that the server may add/update its database of registered clients. This allows the server to acknowledge the transaction and disconnect. In general, the get address transaction is where the client sends an e-mail name so that the server may look up the e-mail name in its database and return the associated IP address (or an error code), then disconnect.

[0039] Still further, the statistics on each transaction may also be recorded in the database, so that a separate administration tool may show the statistics. This allows the administrative tool to detect SPAM attacks on the server, and automatically disable the connections from the offending address.

[0040] As illustrated in FIG. 3, an exemplary user data 56 tracked by the server may include (1) e-mail name; (2) IP address; and (3) date/time of the last connection. Moreover, an exemplary connection data tracked 58 by the server may include (1) originating IP address; (2) count of connections; (3) date/time of last connection; and (4) average milliseconds between connection attempts.

[0041] With regard to a standard SNIP server 54, the bulk of these servers are directed at authentication and registration. Moreover, these servers are responsible for maintaining a database of users that are currently on line. For example, the client may ping the server in a specified amount of time. If the server does not receive a ping from the client in a specified amount of time, then that user's registration may be deleted.

[0042] With regard to the SNIP client 52, it may take on most of the responsibilities of the SNIP protocol and architecture. It may be responsible for negotiating the protocol in its entirety. It plays the main role in the successful execution of the architecture. It handles the other half of the authentication and registration scheme; and may also be responsible for the peer-to-peer communications. It creates ignore, and buddy files on the client's machine, as well as making sure that users on the ignore list are ignored and users on the buddy list are checked for online registration.

[0043] The client may handle requests for communications from other clients. The user has the ability to deny communication requests from other clients or accept them at any time. It is

also the client's responsibility to negotiate the search protocol and complete the searching for another user's connect information from various SNIP servers. It is responsible for pinging the SNIP server to tell the server it is still online and available for communication with other clients. Since the protocol is written in XML, it can be updated easily and new tags can support multiple forms of data, making SNIP clients suitable for voiceover IP and other data messaging technologies. The clients should be expandable and meld with other technologies easily as long as the underlying SNIP protocol remains intact and the authentication process is adhered to.

[0044] FIG. 4 illustrates by way of example a message board to facilitate peer-to-peer instant message communications and/or data communication. For example, the top text box may be for conversation history. The bottom box may be where the user types in the next message it is going to send. Moreover, multiple conversations may be handled by a tab control. There may be an indication when there has been an activity in a tab where the user is not viewing. Although a plain text conversation is illustrated, other textual conversation may look similar. Note that binary data, like files or voices or the net, may need less extensive UI (User Interface).

[0045] Another embodiment of the present invention is to provide a method and system using SNIP that verifies that the rightful owner of a credit card is making an online purchase. To do so, there is a registration process and an authentication process. In the registration process, a simple web form may be provided to enter the credit card information: (1) the credit card number; (2) e-mail address associated with the credit card number; (3) e-mail password for the e-mail address associated with the credit card number; and (4) optionally, bio-password to take a reading of the user's bio-rhythms for the e-mail password. Once the credit card owner has entered the above data and re-enters the e-mail password enough to get a bio-reading of the owner, the data and the bio-reading is sent to a server for storage and registration is complete. Alternatively, many different cryptography techniques and encryption algorithms known to one skilled in the art may be used in the present invention. Once the user has entered this data, the data is sent to the verification server.

[0046] FIG. 5 illustrates by way of example the authentication process of the present embodiment. First, the e-mail address, e-mail password, the bio-rhythmic data, and the credit card number are collected as user data 90. This may be done with a combination of regular HTML form elements. Internet technologies, known to one ordinarily skilled in the art, such as Active X and or Java, may be used to ascertain the bio-rhythmic password logic and read and encode a user's bio-rhythms. The second step is to send the user-data, including bio-rhythmic password data, to the verification server for processing. The server may follow a protocol that has three specific tasks: (1) match the e-mail address to the credit card number given 92; (2) authenticate the user's e-mail address by receiving an authentication from the SNIP protocol 96;

and (3) optionally, authenticate the user's unique bio-rhythm. If all of the above tasks are successful, the verification server will send the merchant data to a gateway for clearing.

[0047] The present embodiment may have two types of authentication: a server side authentication and a client side authentication. Server side authentication is a transaction that the server completes. Simply, the user fills out an HTML form, for example, providing all the information needed to complete a verification. The user's browser sends the information to the verification server via standard HTTP post of gets methods. The server disseminates this information, checks the verification database to make sure the credit card number supplied by the user matches the e-mail address that corresponds to that credit card number in the database. If that succeeds, then the server checks the e-mail address and e-mail password against the POP3 server as in a SNIP authentication. If that succeeds, the transaction is successful.

[0048] Client side authentication may include the steps from the server side, however logic may be downloaded to the browser for the transaction. The client may open a TCP/IP connection with the verification server and complete the transaction as normal in the exact same steps. This makes it possible, for example, to push data to the user at the point of sale.

[0049] There are many ways to integrate SNIP and the bio-rhythmically encoded password authentication of the present embodiment. The authentication steps 1 and 2 may be done by an application service provider or other server side technologies known to one skilled in the art. The SNIP e-mail authentication and the bio-rhythmically encoded password may be integrated into a single combined control. The e-mail and credit card verification service may be completed on the server side, while collecting bio-rhythmic data is performed in a client control and sent to the server for authentication.

[0050] Although the present invention has been described in terms of the preferred embodiments above, numerous modifications and/or additions to the above-described preferred embodiments would be readily apparent to one skilled in the art. For example, besides rhythmic coding the email password, the email address and the credit card number or any other user input may be used as a seed for recording a bio rhythm or any other type of pattern.

[0051] In closing, it is noted that specific illustrative embodiments of the invention have been disclosed hereinabove. With respect to the claims, it is applicant's intention that the claims not be interpreted in accordance with the sixth paragraph of 35 U.S.C. § 112 unless the term "means" is used followed by a functional statement.

WHAT IS CLAIMED IS:

1. A method for authenticating a user to facilitate an instant data communication, comprising the steps of:

receiving an authentication request for a user to a single namespace instant messaging protocol (SNIP) server;

forwarding the authentication request to the user's e-mail protocol; and

receiving a response from the user's e-mail protocol, wherein:

if the response is an ack, then registering the user's IP number with the SNIP server as being ONLINE; and

if the response is a nack, then not registering the user;

whereby all users registered with the SNIP server can receive instant data communication through their e-mail address and/or IP number regardless of Internet Service Provider that the user belongs to, where the communication takes place over a peer-to-peer, client-to-client, or three-tier connection.

2. A method according to claim 1, wherein if the response is an ack, then:

dropping a link with the SNIP server;

opening a socket using the user's IP number to make peer-to-peer communication.

3. A method according to claim 1, wherein the user's e-mail protocol is a Post Office Protocol (POP).

4. A method according to claim 3, wherein the POP is a POP3.

5. A method according to claim 1, wherein:

If the response is an ack, then registering the user's e-mail address with the SNIP server as being on-line.

6. A method according to claim 1, wherein the authentication request is forwarded to the user's e-mail protocol using RFC number 1725.

7. A method according to claim 1, wherein the SNIP server keeps user data.

8. A method according to claim 1, wherein the user data includes:

e-mail name;

IP address;
date of the last connection; and
time of the last connection.

9. A method according to claim 1, wherein the SNIP server keeps connection data.

10. A method according to claim 9, wherein the connection data includes:
originating IP address;
count of connections;
date of last connection;
time of last connection; and
average milliseconds between the connections attempted.

11. A method according to claim 1, wherein the user's e-mail protocol is an Instant Message Access Protocol (IMAP).

12. A method according to claim 1, wherein the instant data communication is a peer-to-peer instant message communication.

13. A method according to claim 1, wherein the instant data communication is voiceover IP.

14. A method according to claim 1, wherein:
if the response is an ack, then pinning a global unique identification (GUID) to the user.

15. A method for a client to look up a user to facilitate an instant data communication, comprising the steps of:
client sending a look-up request for a desired user to a single namespace instant messaging protocol (SNIP) server, wherein the look-up request includes an e-mail address of the desired user;
checking the SNIP server's database for the e-mail address of the desired user; wherein:
if the SNIP server's database has the e-mail address of the desired user, then further including the steps of:

the client receiving the IP address of the desired user stored within the SNIP server's database; and

the client communicating directly with the desired user by opening a socket using the desired user's IP address;

if the SNIP server's database does not have the e-mail address of the desired user, then further including the steps of:

the SNIP server notifying the desired user of the incoming request for connection by sending an e-mail notification to the desired user's e-mail address; and

notifying the client that the desired user is not available.

16. A method for authenticating a credit card used to make an online transaction, comprising:

registering an owner credit card number, an owner e-mail address associated with the owner credit card number, and an owner e-mail password for the owner e-mail address;

checking an e-mail address provided for using the owner credit card number against the owner e-mail address;

checking an e-mail password provided for using the owner e-mail address against the owner e-mail password; and

verifying an online authentication if the checking of e-mail address and the e-mail password match the owner e-mail address and owner e-mail password, respectively.

17. A method according to claim 16, further including:

recording a pattern of the owner e-mail password for an owner of the owner credit card number;

checking an pattern of an e-mail password provided for using the owner e-mail address against the recording of the pattern of the owner e-mail password; and

approving the online transaction if the checking of the pattern matches.

18. The method according to claim 16 wherein the pattern is a bio-rhythmic pattern.

19. The method according to claim 16 further including the steps of:

forwarding the e-mail address to a Single Namespace Instant Messaging Protocol (SNIP) server;

checking the SNIP server's database for the e-mail address; wherein:

if the SNIP server's database has the e-mail address, then the verification server receiving an acknowledgement.

20. A method for authenticating a credit card used to make an online transaction, comprising:

registering a credit card number and a first e-mail address associated with the credit card number, and a first pattern of the first e-mail address;

checking a second e-mail address provided for using the credit card number against the first e-mail address;

checking a second pattern of the second e-mail address provided for using the credit card number against the first pattern of the first e-mail address; and

verifying an online authentication if the first e-mail address is identical to the second e-mail address and if the first pattern is substantially similar to the second pattern.

21. A method according to claim 20 wherein the first pattern and the second pattern are bio-rhythmic patterns.

Figure 1

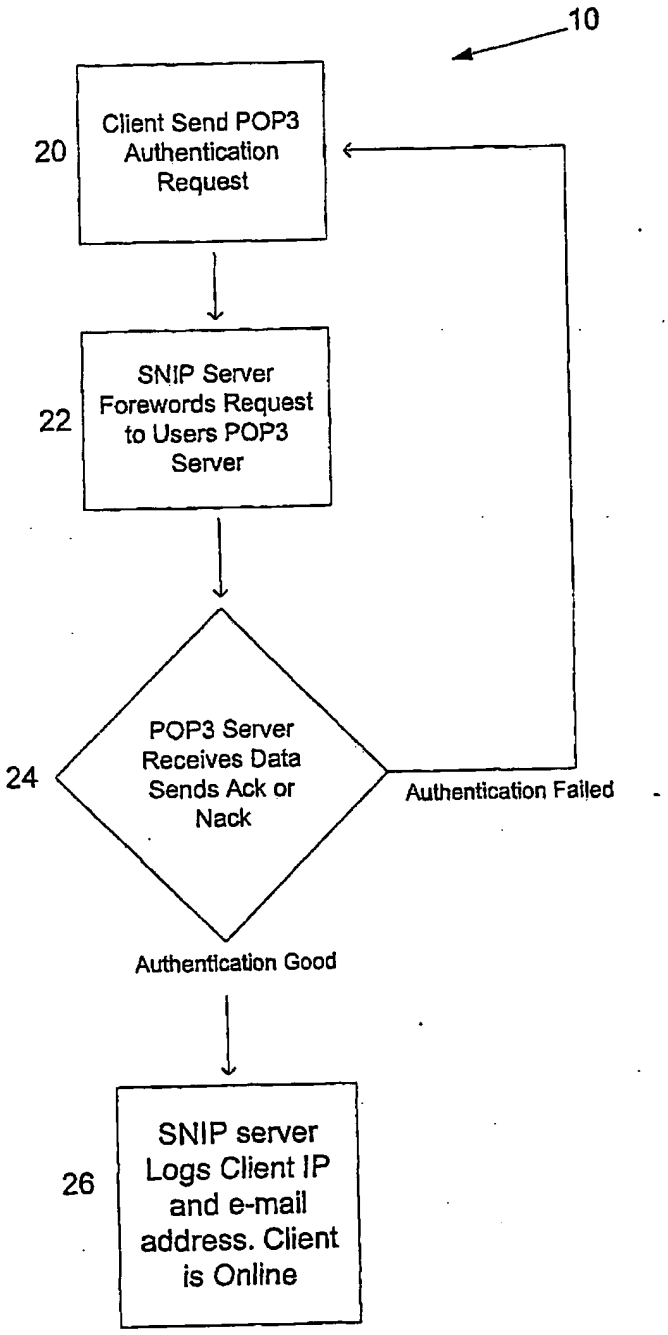

10
20
Client Send POP3 Authentication Request
22
SNIP Server Forewords Request to Users POP3 Server
24
POP3 Server Receives Data Sends Ack or Nack
Authentication Failed
Authentication Good
26
SNIP server Logs Client IP and e-mail address. Client is Online

Figure 2

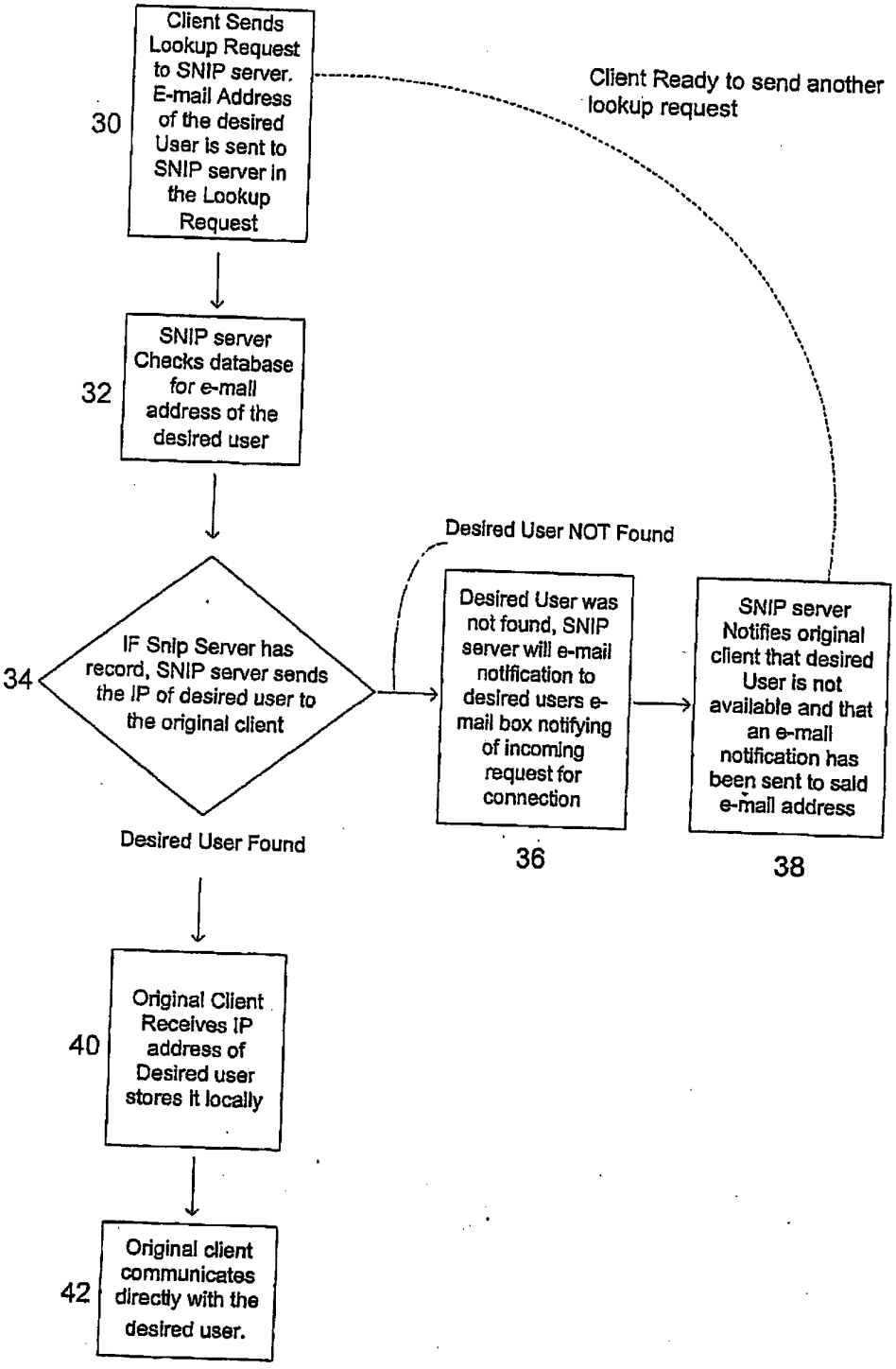
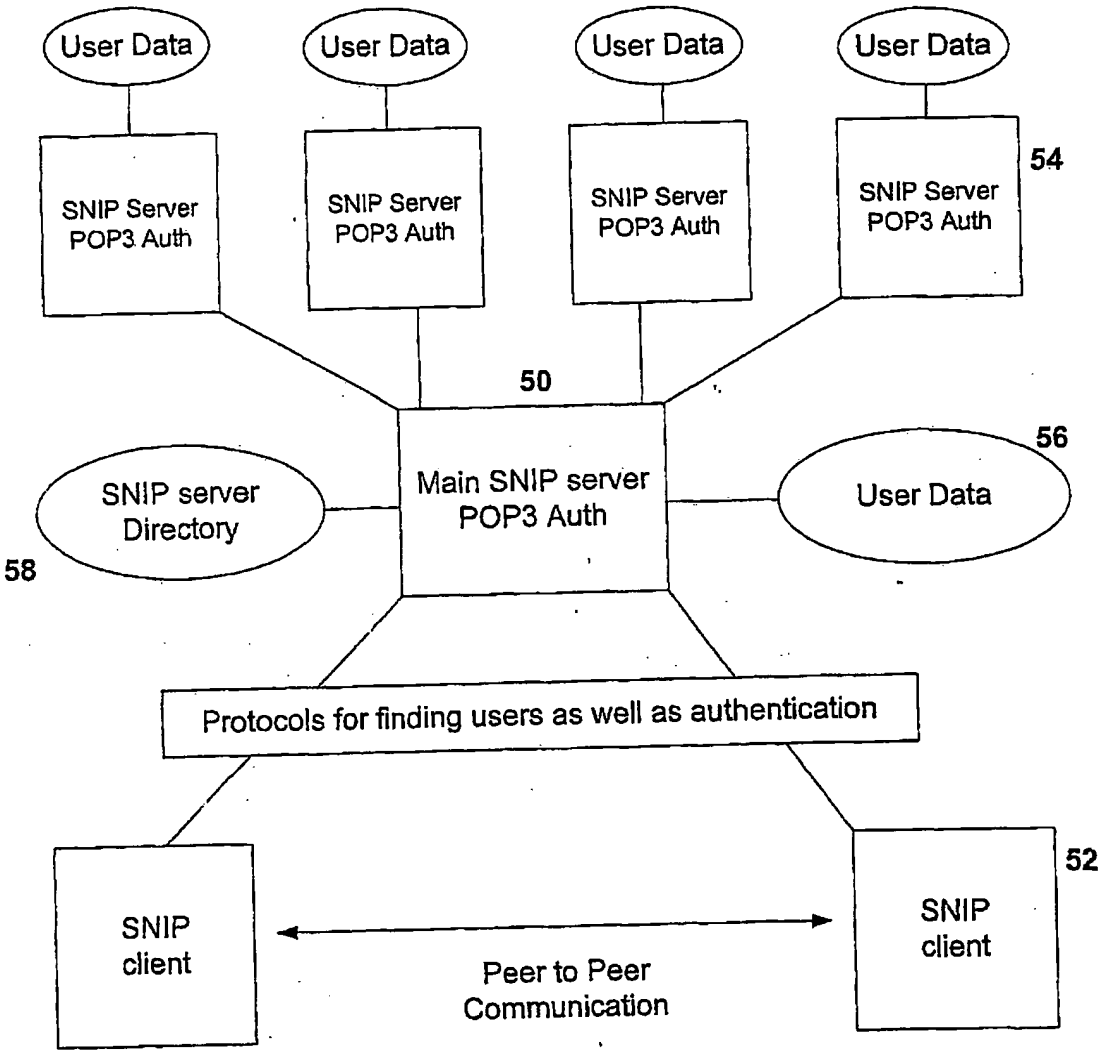
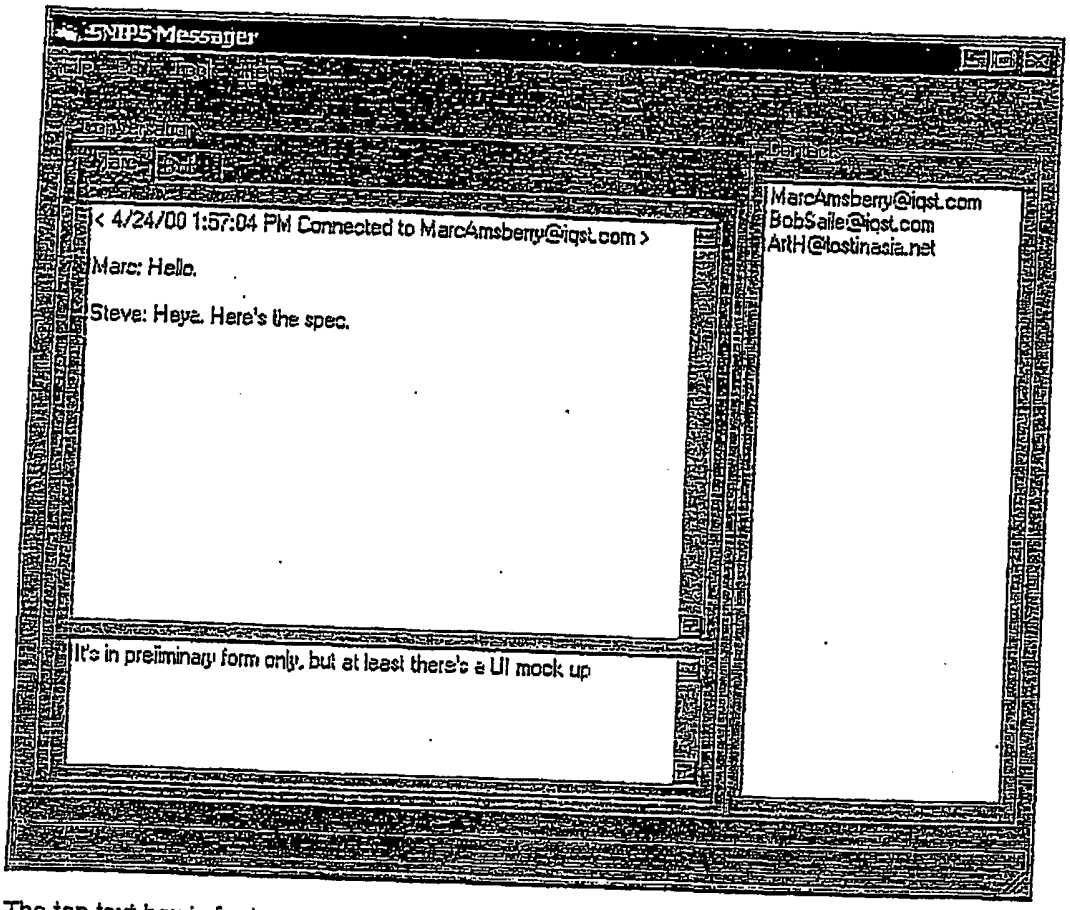

Client Sends Lookup Request to SNIP server. E-mail Address of the desired User is sent to SNIP server in the Lookup Request
30
Client Ready to send another lookup request
SNIP server Checks database for e-mail address of the desired user
32
Desired User NOT Found
IF Snip Server has record, SNIP server sends the IP of desired user to the original client
34
Desired User was not found, SNIP server will e-mail notification to desired users e-mail box notifying of incoming request for connection
36
SNIP server Notifies original client that desired User is not available and that an e-mail notification has been sent to said e-mail address
38
Desired User Found
Original Client Receives IP address of Desired user stores it locally
40
Original client communicates directly with the desired user.
42

Figure 3


User Data
User Data
User Data
User Data
SNIP Server POP3 Auth
SNIP Server POP3 Auth
SNIP Server POP3 Auth
SNIP Server POP3 Auth
54
50
SNIP server Directory
58
Main SNIP server POP3 Auth
56
User Data
Protocols for finding users as well as authentication
SNIP client
Peer to Peer Communication
SNIP client
52

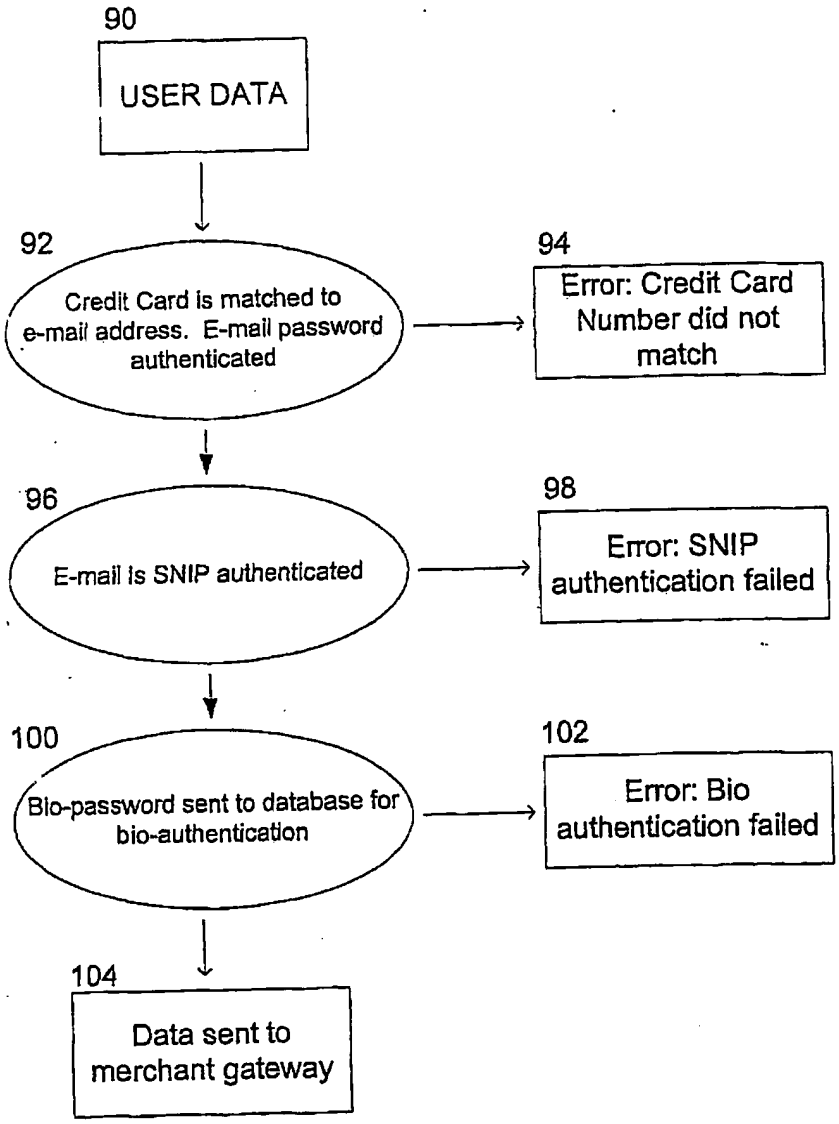
UI Prototype:



The top text box is for 'conversation history'. The bottom is where the user types in the next message they are going to send. Multiple conversations are handled by a tab control. We'll have an indication when there's been activity in a tab you're not viewing. This only shows a 'plain text' conversation, but other textual conversations would likely look similar. Binary data (like files or voice over the net) should need even less extensive UI.

FIG. 4

Figure 5


90
USER DATA
92
Credit Card is matched to e-mail address. E-mail password authenticated
94
Error: Credit Card Number did not match
96
E-mail is SNIP authenticated
98
Error: SNIP authentication failed
100
Bio-password sent to database for bio-authentication
102
Error: Bio authentication failed
104
Data sent to merchant gateway

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 December 2001 (06.12.2001)

PCT

(10) International Publication Number
WO 01/093503 A3

(51) International Patent Classification[7]: H04L 12/18, 12/58, G06F 17/60, H04L 29/06, 9/32, 29/12

(21) International Application Number: PCT/US01/40820

(22) International Filing Date: 31 May 2001 (31.05.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/208,349 31 May 2000 (31.05.2000) US

(71) Applicant *(for all designated States except US)*: SNIP, LLC [US/US]; Suite 1670, 300 Esplanade Drive, Oxnard, CA 93030 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: SPURGIN, Ryan, H. [US/US]; 700 Albany Avenue, Ventura, CA 93004 (US).

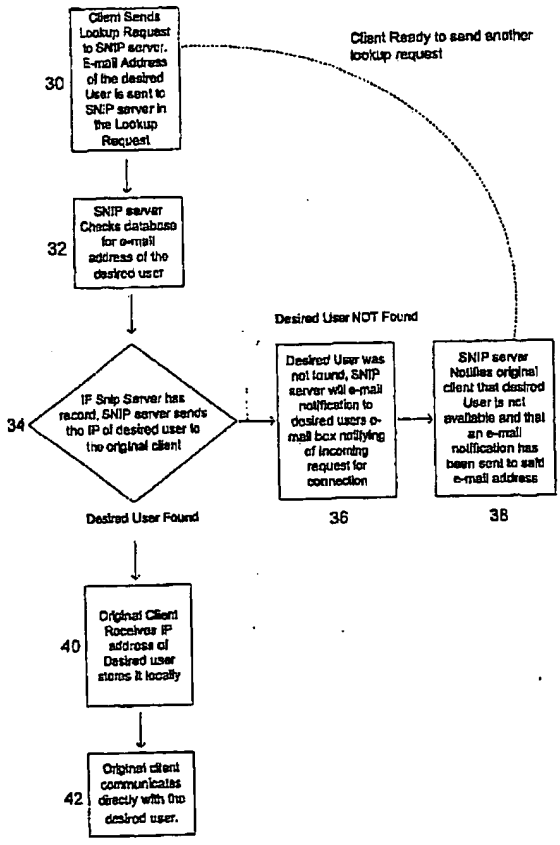
(74) Agents: OH, Sung, I. et al.; Squire, Sanders & Dempsey L.L.P., 14th Floor, 801 South Figueroa Street, Los Angeles, CA 90017-5554 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR INSTANT MESSAGING



(57) Abstract: The present invention provides a method and system to facilitate peer-to-peer instant message communications among users connected to different instant messaging systems. To do so, the present invention provides a Single Name Instant Messaging Protocol (SNIP) that uses the universal namespace of e-mail to facilitate peer-to-peer instant message communications among users connected to different networks. Another aspect of the present invention is to use the Single Name Instant Messaging protocol to authenticate a user over the Internet to provide online fraud protection when using a credit card. To do so, a method and system according to one embodiment of the present invention includes a database that references a credit card number with an e-mail address and its corresponding e-mail password; and, optionally, referencing the same e-mail address to a bio-rhythmically encoded password.

WO 01/093503 A3

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
6 February 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Inte al Application No
PCT/US 01/40820

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/18 H04L12/58 G06F17/60 H04L29/06 H04L9/32
H04L29/12

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	ESCHENBURG A: "Wo laufen sie denn? ICQ hält Verbindung zu Bekannten" CT MAGAZIN FUER COMPUTER TECHNIK, VERLAG HEINZ HEISE GMBH., HANNOVER, DE, no. 22, 26 October 1998 (1998-10-26), pages 92-95, XP000779803 ISSN: 0724-8679 page 93, column 1, line 31 -column 3, line 13	1-15
A	US 5 898 780 A (LIU LYNN Y ET AL) 27 April 1999 (1999-04-27) column 1, line 26 - line 48 column 3, line 32 - last line	1-15

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 March 2002	10. 07. 2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Ströbeck, A

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

ational application No.
PCT/US 01/40820

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-15

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-15

   Method for instant messaging using e-mail address as user identity.

2. Claims: 16-21

   Method for authenticating a credit card used for an on-line transaction.

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter d Application No
PCT/US 01/40820

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5898780 A	27-04-1999	NONE	

Form PCT/ISA/210 (patent family annex) (July 1992)